In the Claims

Please amend the claims to the present application as set forth below. A detailed listing of all claims has been provided. A status identifier is provided for each claim in a parenthetical expression following each claim number.

Claim 1 is currently amended.
Claims 2—36 are as originally filed.
Accordingly, claims 1—36 are pending.

1. (Currently amended.) A method of metering execution of code, comprising:
receiving a call requesting execution of a protected service within a first runtime area;
requesting permission for the execution;
analyzing the request for permission; and
basing status of the permission on the analysis.

2. (Original.) The method of claim 1, wherein the analysis is made within a second runtime area separate from the first runtime area.

3. (Original.) The method of claim 2, wherein the first and second runtime areas reside in different partitions of memory.

4. (Original.) The method of claim 2, wherein the first runtime area is located at a first computing device and the second runtime area is located at a second computing device.

5. (Original.) The method of claim 1, wherein analyzing the request comprises using a contract and meter data as inputs.

6. (Original.) The method of claim 5, additionally comprising updating the meter data to reflect the analysis.

7. (Original.) The method of claim 1, wherein requesting permission comprises opening a secure connection between the protected service and a metering engine configured to perform the analysis.

8. (Original.) The method of claim 1, wherein requesting permission comprises sending an encrypted message from the protected service in the first runtime area to a metering engine within the second runtime area.

9. (Original.) The method of claim 1, wherein the permission was given, additionally comprising:

executing the protected service; and

returning results of the execution to an application that initiated the call.

10. (Original.) The method of claim 1, wherein the permission was not given, additionally comprising returning notice of failure to execute the protected service to an application that initiated the call.

11. (Original.) A processor-readable medium comprising processor-executable instructions for metering execution of code, the processor-executable instructions comprising instructions for:

receiving a request for execution of a protected service;

requesting authorization to execute the protected service, wherein the authorization request is made from the protected service to a metering engine; and

analyzing, with the metering engine, a contract in view of meter data to determine if the authorization request to use the protected service by an application should be allowed.

12. (Original.) The processor-readable medium as recited in claim 11, wherein the metering engine operates within a runtime area that is separate from a runtime area within which the protected service operates.

13. (Original.) The processor-readable medium as recited in claim 11, wherein the analyzing comprises instructions for:

analyzing the contract using the meter data and identity of the protected service as input to an analysis; and

updating the meter data to reflect the analysis.

14. (Original.) The processor-readable medium as recited in claim 11, wherein requesting authorization comprises instructions for opening a secure connection between the protected service and the metering engine.

15. (Original.) The processor-readable medium as recited in claim 11, wherein the metering of code execution is performed in a managed code environment.

16. (Original.) The processor-readable medium as recited in claim 11, additionally comprising, where the authorization request was allowed, instructions for:

executing the protected service; and

returning results of the execution to the application.

17. (Original.) The processor-readable medium as recited in claim 11, additionally comprising, where the authorization request was not allowed, instructions for returning notice of failure to execute to the application.

18. (Original.) The processor-readable medium as recited in claim 11, comprising further instructions for protecting communications between the protected service and the metering engine with cryptography.

19. (Original.) A code-executing device, comprising:

first and second runtime areas with a secure communication channel between them;

a protected service configured to receive a request from an application for execution of the protected service within the first runtime area; and

a metering engine, configured to receive the request and to operate within the second runtime area and to return an allowance code or a rejection code in response to the request by applying rules to meter data.

20. (Original.) The code-executing device of claim 19, wherein the metering engine comprises:

an enforcement engine, configured for secure communication with the protected service;

a service contract, configured to supply the rules governing operation of the protected service, to the enforcement engine; and

a secure store, within which the meter data is contained, wherein the secure store is configured to supply, to the enforcement engine, historical data reflecting past operation of the protected service.

21. (Original.) The code-executing device of claim 19, wherein the metering engine is configured to:

use identity of the protected service and data from a secure store of meter data as input to an analysis providing return of the allowance code or the rejection code; and

update the secure store of meter data to reflect the analysis.

22. (Original.) The code-executing device of claim 19, wherein the code-executing device is a cellular telephone.

23. (Original.) The code-executing device of claim 19, wherein the code-executing device is configured for use within a managed code environment.

24. (Original.) The code-executing device of claim 19, wherein the code-executing device is a compound device, and wherein the protected service is contained on a first portion of the compound device and the metering engine is contained on a second portion of the compound device, and wherein the first portion of the compound device is remotely located from the second portion of the compound device.

25. (Original.) The code-executing device of claim 19, additionally comprising a library of protected services, within which the protected service is contained.

26. (Original.) The code-executing device of claim 19, additionally comprising a library of applications, within which the application is contained.

27. (Original.) A managed code environment, comprising:

an application configured to consume services from a library of protected services;

a protected service, within the library of protected services, configured to receive a request from the application for execution; and

a metering engine, configured to return of an allowance code or a rejection code to the request based on rules governing operation of the protected service.

28. (Original.) The managed code environment of claim 27, wherein the protected service and the metering engine operate within different runtime areas.

29. (Original.) The managed code environment of claim 27, wherein the metering engine comprises:

an enforcement engine, configured for secure communication with the protected service;

a service contract, configured to supply the rules governing operation of the protected service to the enforcement engine; and

a secure store of metered data, configured to supply historical data reflecting past operation of the protected service and the application to the enforcement engine.

30. (Original.) The managed code environment of claim 27, wherein the metering engine comprises:

a service contract containing the rules governing operation of the protected service;

a secure store of meter data; and

an enforcement engine configured to return of the allowance code or the rejection code by:

analyzing the service contract using identity of the application, identity of the protected service, and data from the secure store of meter data as input to the analysis; and

updating the secure store of meter data to reflect the analysis.

31. (Original.) A code-executing device for metering execution of code, the code-executing device comprising:

means for calling a protected service from an application;

means for calling a metering engine from the protected service; and

means for analyzing a contract to determine whether to allow or prohibit use of the protected service by the application.

32. (Original.) The code-executing device as recited in claim 31, additionally comprising, where allowance was determined to be appropriate:

means, defined in the protective service, for executing functionality requested by the application; and

means for returning results of the execution to the application.

33. (Original.) The code-executing device as recited in claim 31, additionally comprising, where rejection was determined to be appropriate, means for returning notice of the rejection to the application.

34. (Original.) The code-executing device as recited in claim 31, wherein the means for analyzing the contract comprises:

means for analyzing the contract using identity of the application, identity of the protected service, rules within the contract, and data from a secure store of meter data as input to the analysis; and

means for updating the secure store of meter data to reflect the analysis.

35. (Original.) The code-executing device as recited in claim 31, wherein the means for calling the metering engine comprises:

means for opening a secure connection between the protected service and the metering engine; and

means for operating the protected service and the metering engine within distinct runtime areas.

36. (Original.) The code-executing device as recited in claim 31, wherein the metering is performed in a managed code environment.